Post-Incident Report Template

Post-Incident Report Template

Post-Incident Report

Incident ID:
[Unique identifier for the incident]

Incident Date and Time:
[When the incident was detected]

Incident Type:
[Type of incident, e.g., Web Application Attack, Data Breach, DDoS]

Incident Impact:
[Summarize the business impact: services disrupted, financial loss, brand reputation damage, etc.]

Duration of Incident:
[Time from detection to full resolution]

Incident Summary:

[A concise overview of what happened, including detection, response, and resolution steps.]

Root Cause Analysis:

[Provide a detailed explanation of the underlying cause of the incident, such as a software vulnerability, human error, lack of proper monitoring, etc.]

Incident Response Review:

- **Was the response timely?** [Yes/No]
- **Did the team follow the incident response plan?** [Yes/No]
- **What worked well during the response?** [List positive aspects of the response]
- **What could have been improved?** [List areas for improvement]

Lessons Learned:

[Discuss what the organization learned from the incident, including the identification of weaknesses, gaps in processes, or tools that can be improved.]

Preventative Measures and Recommendations:

[Based on the root cause and lessons learned, recommend measures to prevent future incidents, such as updating software, strengthening security policies, or providing additional training.]

Action Items for Improvement:

Action	Responsible Person/Team	Target Date
[e.g., Apply patches to critical systems]	[Team/Individual]	[Date]
[e.g., Review and update incident response plan]	[Team/Individual]	[Date]
[e.g., Implement two-factor authentication]	[Team/Individual]	[Date]

Impact on Business Operations:

[Explain in detail how the incident affected business activities, customer trust, revenue, or operations.]

Communication Effectiveness:

[Evaluate how effective internal and external communications were during and after the incident.]

Recovery Time and Cost:

[Outline the time taken to fully recover and the cost of recovery (e.g., financial costs, resource allocation, downtime, etc.)]

Final Resolution:

[State whether the incident has been fully resolved or if further actions are still needed.]

Future Prevention Strategies:

[Summarize the organization's strategy moving forward to prevent similar incidents, including proactive monitoring, vulnerability scanning, employee training, or improved infrastructure.]